



6712-01

FEDERAL COMMUNICATIONS COMMISSION

Privacy Act System of Records

AGENCY: Federal Communications Commission.

ACTION: Notice; one new Privacy Act system of records.

SUMMARY: Pursuant to subsection (e)(4) of the Privacy Act of 1974, as amended (5 U.S.C. 552a), the Federal Communications Commission (FCC or Commission) proposes to add a new system of records, FCC/OMD-30, “FCC Visitors Database.” The FCC’s Security Operations Center (SOC) in the Office of Managing Director (OMD) will use the information contained in FCC/OMD-30 to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (i.e., green card holders), and foreign nationals, must provide to the SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

DATES: In accordance with subsections (e)(4) and (e)(11) of the Privacy Act, as amended, any interested person may submit written comments concerning this new system of records on or before **[INSERT DATE 30 DAYS FROM DATE OF PUBLICATION]**. The Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB), which has oversight responsibility under the Privacy Act to review the system of records, and Congress may submit comments on or before **[INSERT DATE 40 DAYS FROM DATE OF PUBLICATION]**. The proposed new system of records will become effective on **[INSERT DATE 40 DAYS FROM DATE**

OF PUBLICATION] unless the FCC receives comments that require a contrary determination. The Commission will publish a document in the **Federal Register** notifying the public if any changes are necessary. As required by 5 U.S.C. 552a(r) of the Privacy Act, the FCC is submitting reports on this proposed new system to OMB and Congress.

ADDRESSES: Address comments to Leslie F. Smith, Privacy Analyst, Performance Evaluation and Records Management (PERM), Room 1-C216, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, D.C. 20554, or via the Internet at Leslie.Smith@fcc.gov <<mailto:Leslie.Smith@fcc.gov>>.

FOR FURTHER INFORMATION: Contact Leslie F. Smith, Performance Evaluation and Records Management (PERM), Room 1-C216, Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, D.C. 20554, (202) 418-0217, or via the Internet at Leslie.Smith@fcc.gov <<mailto:Leslie.Smith@fcc.gov>>.

SUPPLEMENTARY INFORMATION: As required by the Privacy Act of 1974, as amended, 5 U.S.C. 552a(e)(4) and (e)(11), this document sets forth notice of the proposed new system of records to be maintained by the FCC. This notice is a summary of the more detailed information about the proposed new system of records, which may be obtained or viewed pursuant to the contact and location information given above in the “**ADDRESSES**” section. The purpose for establishing this new system of records, FCC/OMD-30, “FCC Visitors Database,” is for the FCC’s Security Operations Center (SOC) in the Office of Managing Director (OMD) to use this information to cover the personally identifiable information (PII) that all visitors to the FCC, including but not

limited to U.S. citizens, permanent residents (i.e., green card holders), and foreign nationals, must provide to the SOC to gain admittance to the FCC headquarters buildings and other FCC facilities.

This notice meets the requirement documenting the proposed new system of records that is to be added to the systems of records that the FCC maintains, and provides the public, OMB, and Congress with an opportunity to comment.

FCC/OMD-30

SYSTEM NAME:

FCC Visitors Database

SECURITY CLASSIFICATION:

The FCC's Security Operations Center (SOC) has not assigned a security classification to this system of records.

SYSTEM LOCATION:

Office of the Managing Director (OMD), Security Operations Center (SOC), Federal Communications Commission (FCC), 445 12th Street, SW, Washington, D.C. 20554;

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records in this system include all visitors to the FCC. These individuals include, but are not limited to U.S. citizens, permanent residents (i.e., green card holders), and foreign nationals.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records in the FCC Visitors Database include, but are not limited to the individual's first and last name, photographic identification (including but not limited to a driver's license, passport, or other types of photo identification), the authority issuing the photo identification, U.S. visa number, FCC point of contact, visitor signature, professional title, organizational affiliation, contact information for the visitor, including but not limited to wireline and wireless (cell) phone numbers, correspondence related to information required to obtain visitor entry to the FCC, and purpose(s) for visiting the FCC.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 6 U.S.C. 202; 8 U.S.C. 1103, 1158, 1201, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, 1732; Federal Information Security Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); and Federal Property and Administrative Act of 1949, as amended.

PURPOSE(S):

The purpose of the system is to cover the personally identifiable information (PII) that all visitors to the FCC, including but not limited to U.S. citizens, permanent residents (i.e., green card holders), and foreign nationals, must provide to the FCC's Security Operations

Center (SOC) to gain admittance to the FCC headquarters buildings and other FCC facilities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Information about individuals in this system of records may routinely be disclosed under the following conditions:

1. Litigation by the Department of Justice - When: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the FCC or the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ is therefore deemed by the FCC to be for a purpose compatible with the purpose for which the FCC collected the records;
2. Court or Adjudicative Body - In a proceeding when: (a) the FCC or any component thereof; (b) any employee of the FCC in his or her official capacity; (c) any employee of the FCC in his or her individual capacity where the Department of Justice (DOJ) has agreed to represent the employee; or (d) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the FCC determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the FCC to be for a purpose that is compatible with the purpose for which the FCC collected the records;

3. Law Enforcement and Investigation - Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, State, local, tribal, or foreign, or otherwise responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity;
4. Government-wide Program Management and Oversight - When requested by the National Archives and Records Administration (NARA), the Government Accountability Office (GAO), and/or the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. §§ 2904 and 2906 (such disclosure(s)) shall not be used to make a determination about individuals); when the U.S. Department of Justice (DOJ) is contacted in order to obtain that department's advice regarding disclosure obligations under the Freedom of Information Act (FOIA); or when the Office of Management and Budget (OMB) is contacted in order to obtain that office's advice regarding obligations under the Privacy Act;
5. Congressional Inquiries - When requested by a Congressional office in response to an inquiry by an individual made to the Congressional office for the individual's own records;

6. Contract Services, Grants, or Cooperative Agreements - A record may be disclosed to FCC contractors, grantees, or volunteers who have been engaged to assist the FCC in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a;
7. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by the Agency - Disclosure may be made to a Federal, State, local, or tribal government, or other public authority or entity maintaining civil, criminal, intelligence, national security, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the retention of an employee or other personnel action (other than hiring), the retention of a security clearance, the letting of a contract, or the issuance or retention of a grant or other benefit;
8. Employment, Clearances, Licensing, Contract, Grant, or other Benefits Decisions by other than the Agency - Disclosure may be made to a Federal, State, local, or tribal government, or other public authority or entity of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to

another Federal agency for criminal, civil, administrative, personnel or regulatory action;

9. National Security and Intelligence Matters - Disclosure of these records may be made to Federal, State, local agencies, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments and international law enforcement organizations and agencies in order to enable a Federal agency or entity charged with, but not limited to national security and/or intelligence activities and related functions, to carry out these duties and responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable to national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or directives;

10. Department of State, Department of Homeland Security, and other Federal Agencies - A record from this system may be disclosed, where appropriate, to the State Department, Department of Homeland Security (DHS), and/or other Federal agencies and entities charged with, but not limited to national security, law enforcement, immigration, intelligence, and related functions, activities, duties, and responsibilities, where there is an indication of a violation or potential violation of a law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to enforce, investigate, or prosecute violations, or to enforce or implement a statute, rule, regulation, or order issued pursuant thereto, if the

information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving Federal agency or entity;

11. Foreign Governments - A record from this system may be disclosed through the U.S.

Department of State or the Department of Homeland Security (DHS) or other Federal security agencies, entities, or organizations or directly to the representative of such a foreign government or country, to the extent necessary to assist such a government or country in apprehending and/or returning a fugitive to a jurisdiction which seeks the individual's return, or to assist such a country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; and

12. Breach Notification - A record from this system may be disclosed to appropriate

agencies, entities, and persons when: (1) the Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

In each of these cases, the FCC will determine whether disclosure of the records is compatible with the purpose for which the records were collected.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING,
RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

STORAGE:

The information in the FCC Visitors Database includes paper document, files, and records that are stored in file cabinets in the Security Operations Center (SOC), and electronic records, files, and electronic records, files, and data that are stored in the FCC's computer network databases.

RETRIEVABILITY:

The information in the FCC Visitors Database may be retrieved by the name of the individual, driver's license number, U.S. passport number, foreign passport number, U.S. visa number, date of birth (DOB), and/or photo ID number.

SAFEGUARDS:

The paper documents, records, and files are maintained in file cabinets in the SOC's office suite. The file cabinets where these paper documents, files, and records are stored are controlled by on-site personnel when unlocked and locked when not in use. Access to the SOC office suite is through a card-coded main door. Access to the file cabinets is restricted to authorized SOC supervisors, staff, and contractors, whose duties and responsibilities require use of the information.

The electronic records, files, and data are stored in the FCC computer network databases that are secured by limited access card readers. The computer servers themselves are

password-protected. Access to the electronic files is restricted to authorized SOC supervisors, staff, and contractors, and to the Information Technology Center (ITC) staff and contractors, who maintain the FCC's computer network. Other FCC employees and contractors may be granted access on a "need-to-know" basis. The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other security features. A PRIVACY WARNING NOTICE appears on the monitor screen when records containing information on individuals are first displayed. Information resident on the SOC database servers is backed-up routinely onto magnetic media. Back-up tapes are stored on-site and at a secured, off-site location.

RETENTION AND DISPOSAL:

Records in the FCC Visitors Database are retained in accordance with General Records Schedule (GRS) 18, Item 17 approved by the National Archives and Records Administration (NARA). The records disposal is done in accordance with the Commission's disposal policies. Unless retained for specific, on-going security investigations, records of facility access are maintained for one year and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with GRS 18, item 22a, approved by NARA. The records are disposed of in accordance with SOC disposal policies, as follows:

1. All returned day contractor cards will be reused on a daily basis.

2. Transaction data for all FCC Visitors Database cards will be stored using a secure medium and retained for one year in the SOC, which is locked and secured with an alarm system.

In accordance with Homeland Security Presidential Directive (HSPD-12), Personal Identity Verification (PIV) Cards are deactivated within eighteen (18) hours of notification of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with GRS 11, Item 4. PIV Cards are destroyed by burning in an approved Federal burn-facility.

SYSTEM MANAGER(S) AND ADDRESS:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, D.C. 20554.

NOTIFICATION PROCEDURE:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

RECORD ACCESS PROCEDURES:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

CONTESTING RECORD PROCEDURES:

Security Operations Center (SOC), Office of Managing Director (OMD), Federal Communications Commission (FCC), 445 12th Street, S.W., Washington, DC 20554.

RECORD SOURCE CATEGORIES:

The sources for information in this system are the visitors themselves and/or their agency or organizational sponsor(s) who have been invited to or have requested admittance to the FCC headquarters buildings and other FCC facilities for the visitors.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Federal Communications Commission.

Marlene H. Dortch,

Secretary,

Office of the Secretary,

Office of Managing Director.

[FR Doc. ??-????? Filed ??-??-??; 08:45 am]

BILLING CODE 6712-01-P

[FR Doc. 2012-12949 Filed 05/29/2012 at 8:45 am; Publication Date: 05/30/2012]